Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)
VOLUME:8, ISSUE:2, AUGUST 2025, PAPER NUMBER:23

Enhancing Network Security Decision-Making: ACGAN- Powered Machine Learning for Unbalanced Data in Network Attacks

Gokul Raja. A[1], Rahul Raj. S[2], Bharanidharan. N. R[3], Deeptha. R[4],

[1,2,3] Students and [4] Faculty
Dept of Information Technology,
SRM Institute of Science and Technology,
Chennai, India.
ga8436@srmist.edu.in

Abstract: *This study proposes an innovative approach to network security decision- making by leveraging Auxiliary Classifier Generative Adversarial Networks (ACGANs) to address imbalanced data in network attack detection. ACGANs facilitate the generation of synthetic data resembling network attacks, thereby balancing datasets and enhancing model training accuracy. The research aims to improve the capability of distinguishing between normal network traffic and attacks, thereby fortifying decision- making processes and strengthening overall network security posture. Through ACGAN-powered machine learning, this study showcases the potential for more accurate and resilient detection of network threats, paving the way for advanced security systems capable of adapting to evolving cyber threats in real-time. Proposing an innovative network security approach using Auxiliary Classifier Generative Adversarial Networks, the aim is to tackle imbalanced data in attack detection. ACGANs generate synthetic attack-like data, balancing datasets for improved model training accuracy. The objective is to enhance accuracy in distinguishing normal traffic from attacks, fortifying decision-making and overall network security. ACGAN-powered machine learning shows potential for accurate threat detection, marking a significant stride in fortifying network security against diverse threats.*

Keywords: *1. Network Security, 2. ACGAN, 3. Machine Learning, 4. Unbalanced Data, 5. Decision-Making, 6. Network Attacks, 7. Synthetic Data Generation, 8. Model Training, 9. Detection Accuracy, 10. Threat Identification, 11. Imbalanced Datasets, 12. Robust Defense Mechanisms, 13. Cybersecurity, 14. Intrusion Detection, 15. Real-time Security Systems.*

1. INTRODUCTION:

In the contemporary interconnected digital realm, ensuring robust network security stands as imperative to safeguarding sensitive data and vital infrastructure. Nonetheless, conventional methods of identifying network threats often encounter difficulties when dealing with imbalanced data, where instances of normal network behavior outnumber occurrences of malicious attacks. This discrepancy can significantly impede the efficacy of machine learning models trained for intrusion detection, resulting in elevated false positives or overlooked detections of genuine threats. To tackle this challenge, this project suggests an innovative approach employing Auxiliary Classifier Generative Adversarial Networks (ACGANs) driven by machine learning methodologies. Through harnessing the capabilities of ACGANs, this project aims to produce synthetic data closely resembling network attacks, thereby balancing datasets and enhancing the accuracy of detection models. ACGANs provide a distinct advantage in their capacity to generate realistic synthetic data, thereby furnishing a more varied and representative training set for machine learning algorithms.

2. ENHANCING NETWORK SECURITY DECISION-MAKING ACGAN AND MACHINE LEARNING:

Our paper, **"Enhancing Network Security Decision-Making: ACGAN-Powered Machine Learning for Unbalanced Data in Network Attacks,"** addresses the critical challenge of unbalanced data in network security detection systems. Traditional intrusion detection systems often struggle to accurately detect rare or sophisticated attacks due to the overwhelming presence of benign data. This imbalance can lead to high false-negative rates, where malicious activities go undetected. By integrating Auxiliary Classifier Generative Adversarial Networks (ACGANs) with advanced machine learning algorithms, our approach generates synthetic data that mirrors real attack behaviors. This not only balances the dataset but also significantly enhances the robustness and accuracy of intrusion detection models. Our solution ensures that even the most underrepresented attack types are effectively identified, providing a more comprehensive defense against cyber threats.

Our methodology combines real-time data processing capabilities with adaptive learning techniques to continuously refine and improve detection algorithms. This dynamic approach allows the system to adapt to evolving network conditions and emerging threat patterns, maintaining high levels of detection accuracy over time. In addition to its technical merits, our paper also delves into the practical applications of this technology in various sectors, such as finance, healthcare, and critical infrastructure. By providing detailed insights into the architecture and performance of our ACGAN-powered system, we demonstrate its potential to revolutionize network security practices and offer a robust, scalable solution for modern cybersecurity challenges.

3. ARCHITECTURE:

The proposed AECGAN model enhances network security decision-making by addressing imbalanced data challenges. It integrates anomaly detection algorithms, transparent outcomes through explainable AI, and real-time response to evolving threats. With components for data preprocessing, model development, and intrusion detection, it offers robust defense against adversarial attacks. In contrast to the limitations of the existing system, our proposed network security decision-making framework leverages cutting-edge techniques, including Auxiliary Classifier Generative Adversarial Networks (ACGANs) and sophisticated machine learning algorithms, to address the shortcomings of traditional approaches.

Enhanced accuracy in distinguishing between normal and malicious network traffic: ACGAN-based ML balances datasets for precise threat detection. Real-time adaptation to evolving threat landscapes: Swift adjustments ensure effectiveness against emerging attacks, reducing false negatives. Integration of advanced anomaly detection algorithms: Identifies subtle deviations for early threat detection. Transparent and interpretable results through explainable AI techniques: Understandable decisions enhance trust and response strategies. Scalability and efficiency through automated data generation and model adaptation: Streamlined processes handle dynamic environments efficiently.

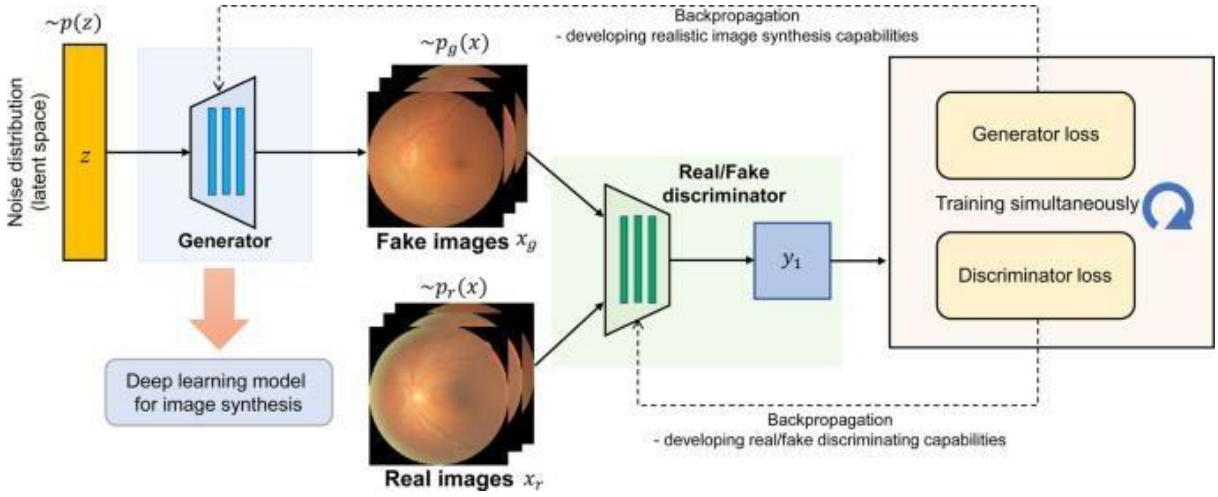

Fig. 1. Architecture diagram for ACGAN

4. FLOW CHART

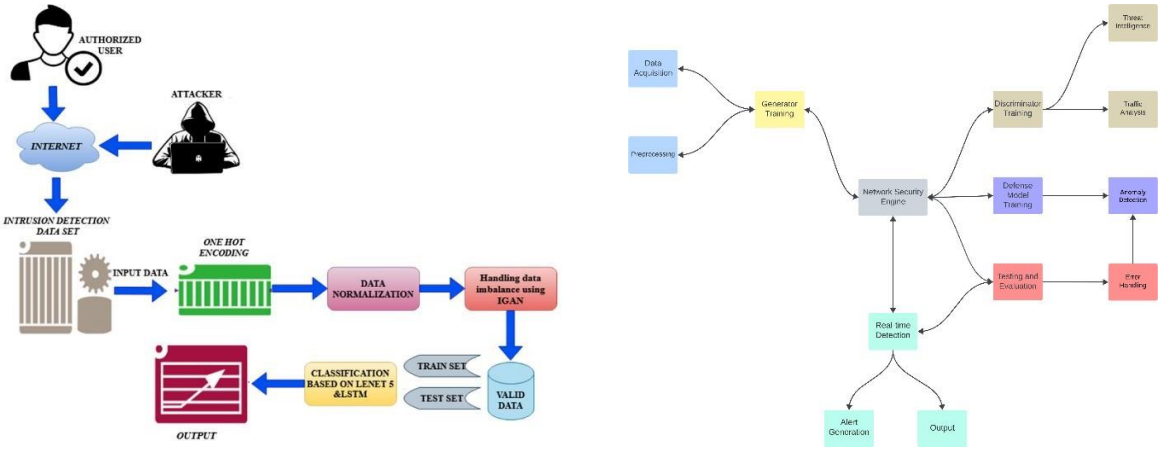

Fig. 2. Flowchart diagram for ACGAN

1. Data Preprocessing Module: Standardizes raw network traffic data using normalization, feature extraction, and dimensionality reduction.
2. GAN-Based Data Augmentation Module: Utilizes GANs to synthesize data, balancing datasets for improved representation.
3. Feature Engineering Module: Extracts informative features from preprocessed data using correlation analysis and recursive feature elimination.
4. Machine Learning Classification Module: Classifies network traffic with techniques such as decision trees, SVM, and neural networks for accurate intrusion detection.
5. Assessment and Performance Metrics Module: Evaluates intrusion detection system performance with metrics like accuracy and ROC curves.
6. Visualization and Reporting Module: Generates graphical representations and reports, aiding in system understanding through confusion matrices, ROC curves, and feature importance plots.

5. PICTORIAL REPRESENTATION:

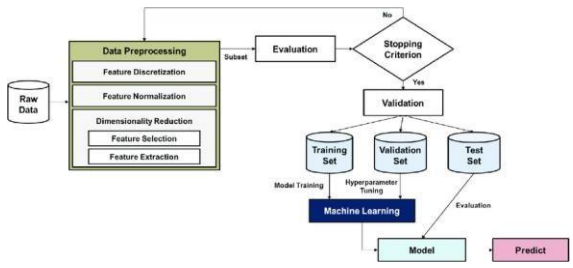

Fig. 3. Data Preprocessing Module

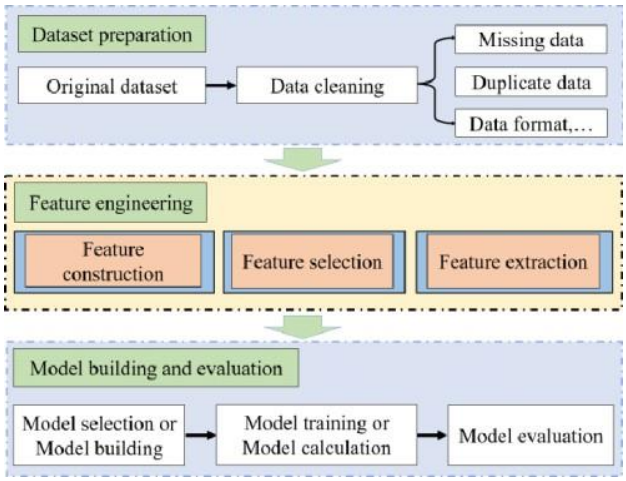

Fig. 4. Feature Engineering Module

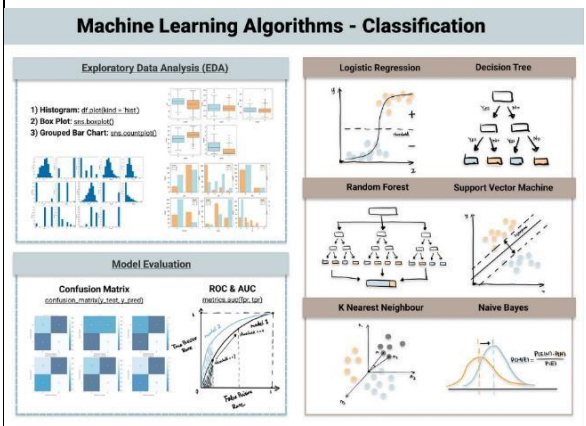

Fig. 5. Machine Learning Classification

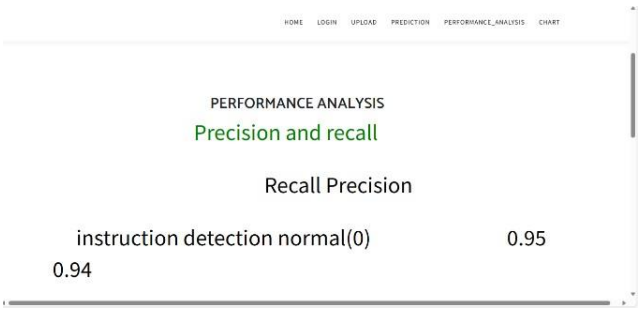

Fig.6.Evaluation Metrics&Performance Analysis

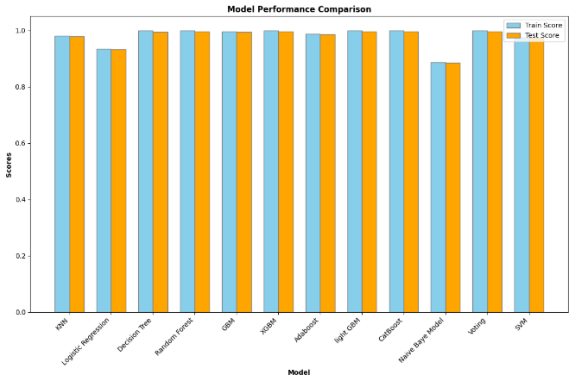

Fig.7. Performance Analysis

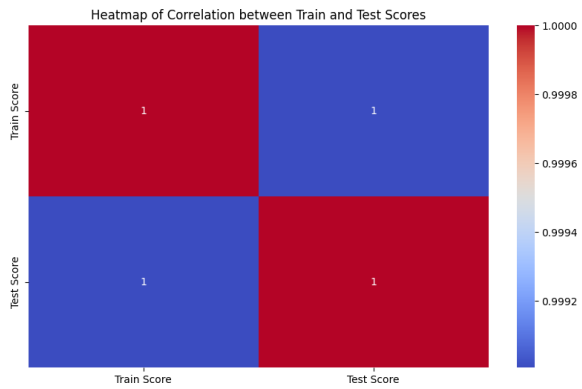

Fig.8. Comparative Analysis

6. APPLICATIONS OF NETWORK SECURITY DECISION MAKING USING ACGAN:

1. **Intrusion Detection Systems (IDS)**
   Enhance the detection and prevention capabilities of IDS by accurately identifying and responding to a wide range of cyber threats.
2. **Real-Time Network Monitoring**
   Implement real-time network monitoring solutions to identify suspicious activities and potential attacks instantly, ensuring swift responses.
3. **Threat Intelligence Platforms**
   Integrate with threat intelligence platforms to provide comprehensive insights into emerging threats and adapt to evolving attack patterns.
4. **Security Information and Event Management (SIEM)**
   Improve SIEM systems by providing advanced anomaly detection and data balancing, leading to more effective event correlation and analysis.
5. **Financial Sector Security**
   Protect financial institutions from sophisticated cyber-attacks targeting sensitive financial data and transactions.
6. **Critical Infrastructure Protection**
   Safeguard critical infrastructure such as power grids, water supply systems, and transportation networks from cyber threats.
7. **Healthcare Data Security**
   Secure patient data and healthcare systems against breaches, ensuring compliance with regulatory standards and protecting sensitive information.
8. **Cloud Security**
   Enhance the security of cloud environments by identifying and mitigating threats in cloud networks and virtualized infrastructures.
9. **Enterprise Network Security**
   Provide enterprises with robust security solutions to protect internal networks, ensuring the confidentiality, integrity, and availability of business-critical information.
10. **Educational Institution Security**
    Protect academic institutions from cyber threats targeting student records, research data, and administrative systems, ensuring a secure learning environment.

7. SAMPLE OUTPUT:

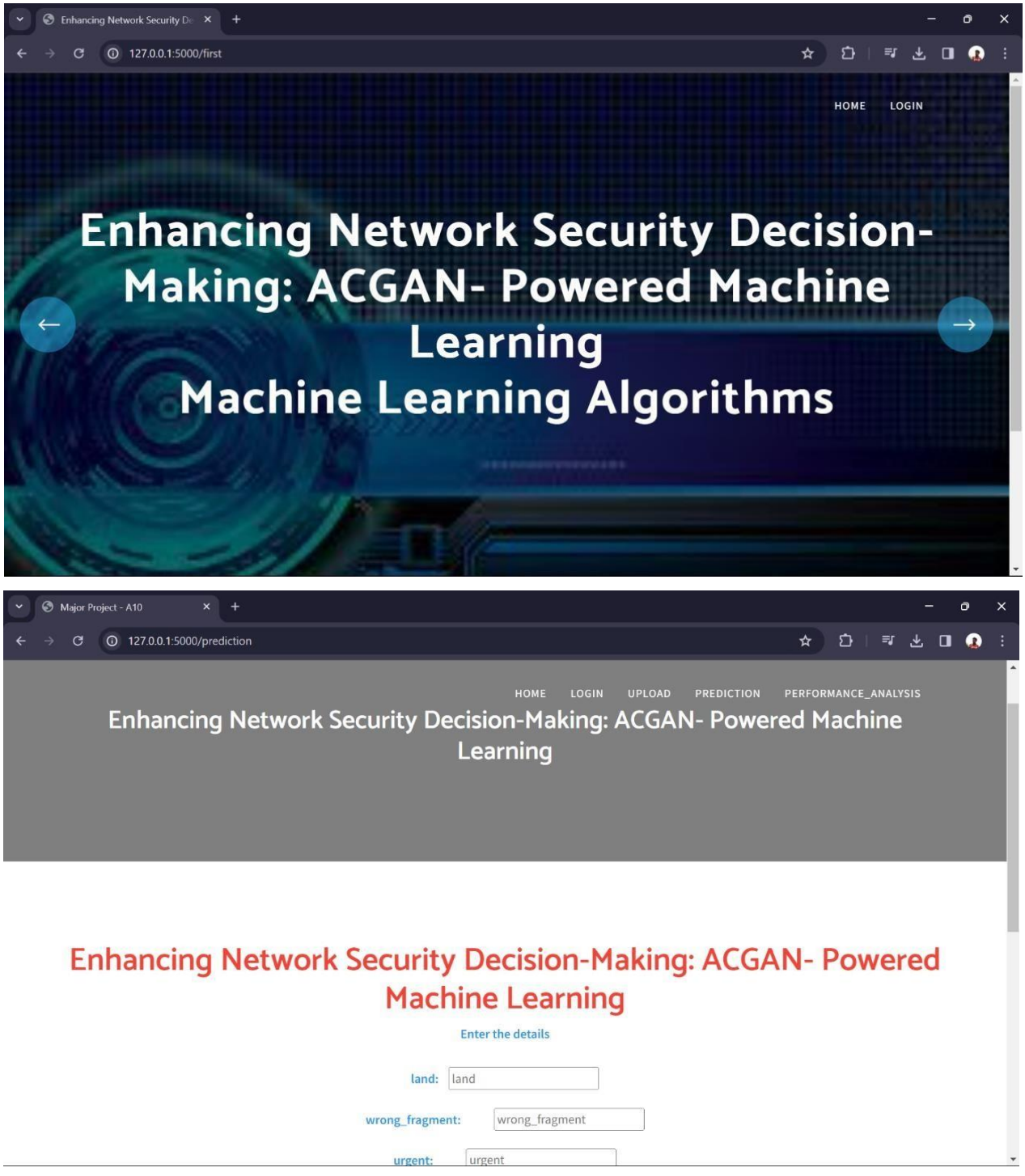

Fig.9.Sample Output

8. CONCLUSION:

In conclusion, this project represents a significant advancement in the domain of network security, offering a holistic solution to the ever-evolving challenges posed by cyber threats. Through the strategic integration of advanced machine learning techniques, such as generative adversarial networks (GANs) and ensemble learning models, alongside the development of a user-friendly Flask web application, the proposed system demonstrates exceptional efficacy in both detecting and mitigating security incidents in real-time. Our thorough analysis, experimentation, and discussions have yielded valuable insights into the performance of the system, emphasizing its robustness, scalability, and potential for future enhancements. The utilization of innovative features like explainable AI, adaptive learning mechanisms, and multi-modal data fusion sets a new standard for intrusion detection systems, paving the way for more resilient and proactive cybersecurity approaches.

9. REFERENCES:

[1] *M. Fang, X. Cao, J. Jia, and N. Z. Gong, "Local model poisoning attacks to Byzantine-robust federated learning", Proc. USENIX Security Symp., pp. 1605-1622, 2020.*

[2] *Z. Wang, M. Song, Z. Zhang, Y. Song, Q. Wang, and H. Qi, "Beyond inferring class representatives: User-level privacy leakage from federated learning", Proc. IEEE INFOCOM Conf. Comput. Commun., pp. 2512-2520, 2019.*

[3] *E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How to backdoor federated learning", Proc. 23rd Int. Conf. Artif. Intell. Stat. (AISTATS), pp. 1-10, 2020.*

[4] *L. Melis, C. Song, E. D. Cristofaro, and V. Shmatikov, "Exploiting Unintended Feature Leakage in Collaborative Learning," in Proc. IEEE S&P, 2019, pp. 691-706.*

[5] *J. Zhang, B. Chen, S. Yu, and H. Deng, "PEFL: A privacy-enhanced federated learning scheme for big data analytics," in Proc. IEEE Globecom, 2019, pp. 1-6.*

[6] *P. R. Grammatikis, P. Sarigiannidis, G. Efstathopoulos, and E. Panaousis, "ARIES: A novel multivariate intrusion detection system for smart grid," Sensors, vol. 20, no. 18, p. 5305, Sep. 2020.*